



February 22, 2016

Mr. Christopher Kirkpatrick  
Secretary of the Commission  
Office of the Secretariat  
Commodity Futures Trading Commission  
3 Lafayette Centre  
1155 21st Street, N.W.  
Washington D.C. 20581

**RE: Nadex Comment Regarding System Safeguards Testing Requirements**

Dear Mr. Kirkpatrick,

The North American Derivatives Exchange, Inc. (“Nadex” or the “Exchange”) is a retail focused derivatives clearing organization (“DCO”) and designated contract market (“DCM”) registered with the Commodity Futures Trading Commission (the “Commission”), offering binary options and spread contracts. Nadex is grateful for the opportunity to comment on the Commission’s proposed regulations pertaining to enhanced cybersecurity requirements for designated contract markets (“DCMs”) and derivatives clearing organizations (“DCOs”), as set forth in the Federal Register 80, No. 246, at 80113 and 80139.

The sophistication level and growing number of cyberattacks financial institutions face is increasingly concerning, and therefore the implementation of a regulatory regime addressing cybersecurity at this time is apropos. Nadex commends the Commission’s undertaking of this endeavor. Nadex supports the Commission’s efforts to clarify and enhance its current security regulations, align its requirements with the industry standards, and to ensure its registrants are meeting thresholds for compliance. Nadex agrees with the general thrust of the proposed regulations, but would request additional clarification or consideration of certain aspects of the regulations. This letter breaks out each proposed regulation, along with Nadex’s comments and concerns relating to each proposal. As the Commission has proposed parallel regulations for DCMs and DCOs, and as Nadex is both a registered DCM and DCO, this comment is intended to address both proposals.

**Vulnerability testing:** Nadex agrees generally with the proposed regulation, however, would like confirmation that the expected level of detail contained in the risk assessment test used to determine the frequency of overall testing should be based on what is considered reasonable in the industry.

North American Derivatives Exchange, Inc., 311 South Wacker Drive, Suite 2675, Chicago, IL 60606

US Toll-Free +1 (877) 77 NADEX info@nadex.com www.nadex.com

**Penetration Testing, Controls Testing, Security and Incident Response Plan Testing:** Nadex generally agrees with these proposed regulations and has no specific comments or concerns in this respect.

**Enterprise-wide Assessment of Risk Management:** Nadex agrees with the proposed regulation generally, but requests the Commission confirm that the information required of this regulation could be combined with the regular testing results presented to management and the Board in the internal reporting and review requirements proposed below, or if it must exist as a stand-alone assessment.

In addition to the specific testing requirements set forth above, the Commission proposes the following additional testing-related risk analysis and oversight requirements:

**Scope of Testing:** The Commission’s proposed “Scope of Testing and Assessment” requires the firm to “include all testing of automated systems and controls necessary to identify *any* vulnerability which, if exploited or accidentally triggered, could enable an intruder or unauthorized user or insider to interfere with the entity’s operations or with fulfillment of its statutory and regulatory responsibilities; to impair or degrade the reliability, security, or capacity of the entity’s automated systems; to add to, delete, modify exfiltrate, or compromise the integrity of *any* data related to the entity’s regulated activities; or to undertake *any* other unauthorized action affecting the entity’s regulated activities or in the hardware or software used in connection with those activities”<sup>1</sup> [*emphasis added*], and further that the testing scope should consider “the nature of the organization’s possible adversaries and their capabilities as revealed by current cybersecurity threat analysis.” While Nadex agrees with the proposed scope generally, it contends that the requirement to identify “any vulnerability” that could compromise “any data”, or “any other unauthorized action” is far too broad. It is unrealistic, and likely impossible, to guarantee testing that could provide 100% security of data against any vulnerability or unauthorized action. Nadex requests that the proposed requirement be amended to limit responsibility to a reasonableness standard. Additionally, the “current cybersecurity threat analysis” the organization would use to assess its possible adversaries’ capabilities could be interpreted not only as the organization’s internal risk assessment, but also include warnings/notices generated from third party entities. Nadex requests the Commission to confirm that the “current cybersecurity threat analysis” refers only to the organization’s internal risk assessment.

**Internal Reporting and Review of Test Results:** The Commission’s proposal states that management and the Board should “receive and review reports of the results of all testing and assessment”. Reports generated based on system testing are often lengthy and technical. Requiring management and the Board to review technical testing results would require individuals in those positions to have a level of technical knowledge and sophistication that may not otherwise be required of the position. Nadex requests the Commission confirm whether the actual testing reports

---

<sup>1</sup> 80 Fed. Reg. 80159 (December 23, 2015).

should be provided to management and the Board, or if a narrative executive summary of the results is sufficient.

Additionally, Nadex requests the Commission confirm that the reports may be presented to the Board at its regularly scheduled quarterly meetings.

**Remediation of Vulnerabilities and Deficiencies Revealed by Testing:** The Commission's "Remediation" proposal would require analyzation of the testing and assessment results "in order to identify *all* vulnerabilities and deficiencies in its systems"<sup>2</sup> [*emphasis added*]. Nadex agrees with the proposed remediation requirements generally, however, the language requiring identification of "all" vulnerabilities and deficiencies would essentially impose strict liability on the firm for any breach of its security. Such a standard would be virtually impossible to comply with, and would place an unreasonable burden on entities subject to the regulation. It appears from later discussion regarding the industry best practices that the Commission's intent was to require remediation of vulnerabilities and deficiencies identified in the testing results, in which case, it is suggested that the language of the proposed regulation be amended to reflect that intent.

Without minimizing the importance of preventative measures such as ongoing testing and analysis, and regular communication with senior managers and the Board, it is impossible for any institution to accurately predict all potential threats its systems may face or provide a 100% secure system. Commissioner Giancarlo recognized that those "who abide by the rule should not be afraid of a 'double whammy' of a destructive cyber-attack followed shortly thereafter by a CFTC enforcement action."<sup>3</sup> Nadex urges the Commission to establish safe harbor provisions offering protection where it is apparent the firm has acted in good faith and maintains reasonable standards, consistent with at least the minimum requirements proscribed by the regulations, to prevent, monitor, detect, and address internal and external cyber threats. Given the differences among each firm, a one-size-fits-all mandate is not the most effective means to accomplish the goals of the proposals. Compliance with the regulations will be a subjective review, and accordingly it is imperative that the Commission provide clear guidelines for safe harbor eligibility.

Thank you for consideration of these comments, and please do not hesitate to contact us should you have any questions in this regard.

Sincerely,



Timothy G. McDermott  
Chief Executive Officer

---

<sup>2</sup> *Id.* at 80160.

<sup>3</sup> *Id.* at 80191.